МЕТОД ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БАЗЕ ПРИКАЗОВ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ №66 И №130

Шиш Д.Н.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Половеня С.И. – канд. техн. наук

В данной работе рассмотрена характеристика типичных атак на информационную структуру предприятия, а также реализация предложенного варианта методика оценки защищённости на базе приказов Оперативно-аналитического центра при Президенте Республики Белаурсь №66 и №130, сюда же входит обзор программного средства для реализации данных задач.

В современном мире цифровизация объектов информационной инфраструктуры все более реализуются в виде взаимного проникновения информационной потоков информационных систем (далее – ИС) различного назначения, которые имеют недостатки или чувствительные места в используемом системном и (или) прикладном программном обеспечении, в том числе в программно–аппаратных средствах, называемые уязвимостями. Уязвимости используются злоумышленниками для проведения различного рода кибератак. Вектор действия кибератаки разграничивает их на направленные(таргетированные) и ненаправленные(массовые).

Массовыми являются кибератаки, которые действуют на широкий круг пользователей. Как правило – это вредоносное программное обеспечение, эксплуатирующее распространенные уязвимости в программном обеспечении, которые, внедрившись в слабозащищенную (чувствительную) ИС, несанкционированно воздействуют на информационные ресурсы ИС. В качестве целей кибератак могут быть рассмотрены: получение прибыли, получение доступа к конфиденциальной информации, ограничение доступа легитимным пользователям и тому подобное. Средствами достижения целей кибератак являются, но не ограничиваются: мошенничество, распространение ботнета, внедрение майнера. Ввиду того, что вредоносное программное обеспечение, распространяемое в информационной сети, действует на широкий круг потенциальных жертв и давно известны используемые ими алгоритмы воздействия, а также сигнатуры такого программного обеспечения – выстроилась успешная практика борьбы с подобными кибератаками, например, блокировка известных источников распространения вредоносного программного обеспечения и применение типовых средств защиты информации.

Таргетированные кибератаки отличаются от массовых тем, что в них злоумышленник заранее определяет жертву, а потому, при планировании кибератаки, разрабатывает уникальные вариации вредоносного ПО, использует уязвимости нулевого дня, придерживается различных подходов для успешного проведения кибератаки (разведка, проникновение, распространение). Цели данных кибератак зачастую направлены на получение несанкционированного доступа к конкретному хосту (сети) с целью получения доступа к информации для последующего её распространения, шантажа, нелегитимной модификации. Обнаружить и предотвратить подобные кибератаки путем использования средств защиты информации, анализирующие программного обеспечение на наличие общеизвестных сигнатур – невозможно. Для борьбы с таким типом кибератак, следует проводить оценку защищённости информационной инфраструктуры предприятия.

Существует множество критериев, которые в своей совокупности решают задачу обеспечения информационной безопасности предприятия. В их числе выбор актуальных сертифицированных средств защиты информации, корректная настройка серверного и сетевого оборудования, проведение как внешнего, так и внутреннего аудита информационной инфраструктуры предприятия, а также строгое соответствие законодательству РБ в области защиты информации и обеспечения кибербезопасности.

Для оценки соответствия СЗИ законодательству РБ разработано программное обеспечение, в основе которого стоят приказы Оперативно-аналитического центра при Президенте Республики Беларусь № 66 и № 130. Алгоритм приложения основан на анкетировании, сборе информации об используемых средствах и реализованных методах защиты информации на предприятии с последующей оценкой уровня защищенности и формированием рекомендаций. Данное программное обеспечение автоматизирует процесс сбора данных для специалиста по ЗИ, а также решает задачу по

упрощению формирования отчёта о степени защищённости и предупреждения о возможных угрозах информационной безопасности информационной структуре предприятия Заказчика.

При использовании данного программного обеспечения в совокупности с другими программными решениями в процессе проведения аудита ИБ позволит достичь более точного представления о степени защищённости информационной инфраструктуры предприятия, построить вектор атаки и определить модели возможных злоумышленников, оценить риски ИБ и возможные решения для корректирования мер обеспечения ИБ для достижения высокого уровня защиты информационной структуры.